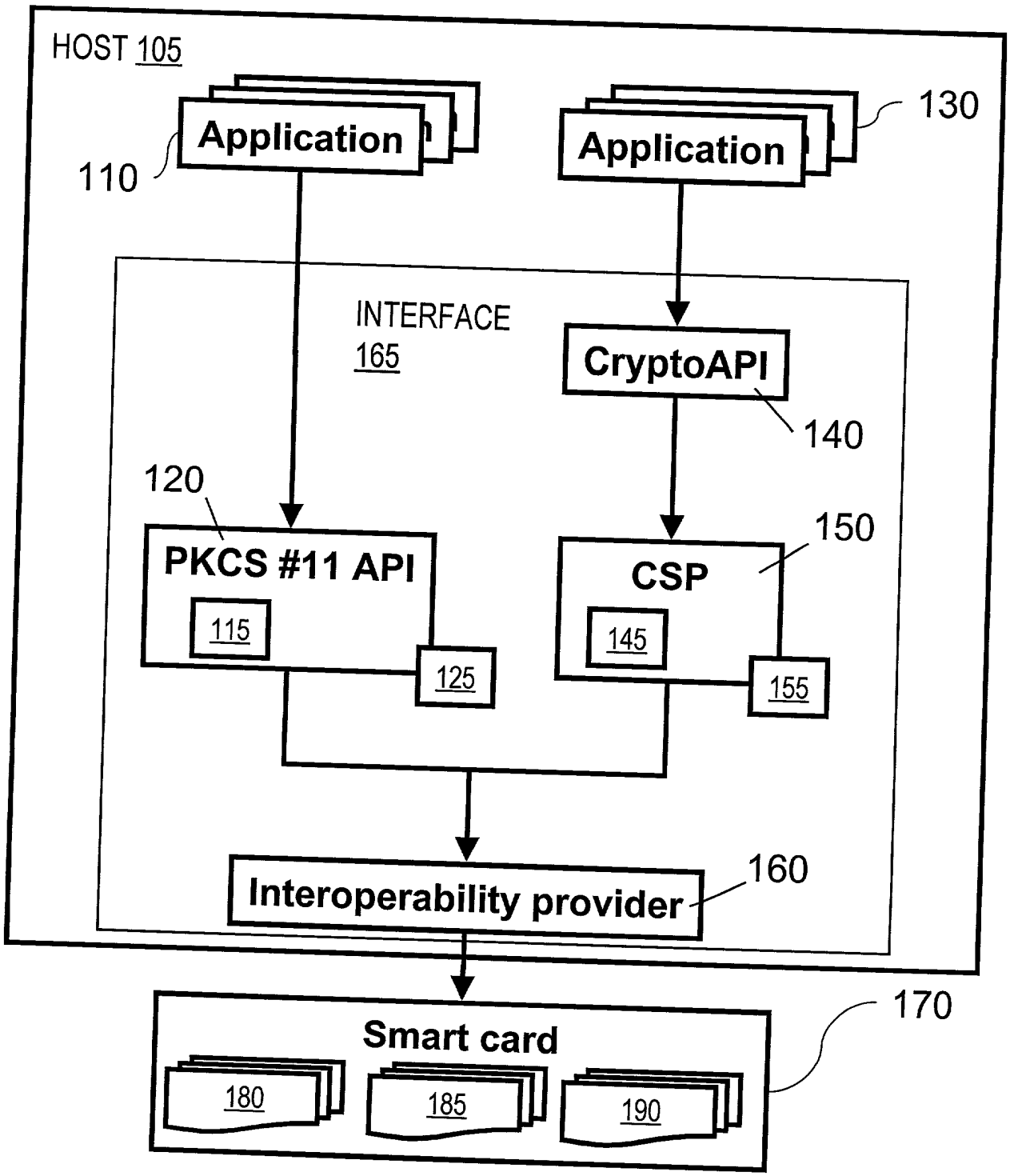
HOST 105
Application
110
Application
130
INTERFACE
165
CryptoAPI
140
120
PKCS #11 API
115
125
150
CSP
145
155
Interoperability provider
160
Smart card
170
180
185
190

FIG. 1

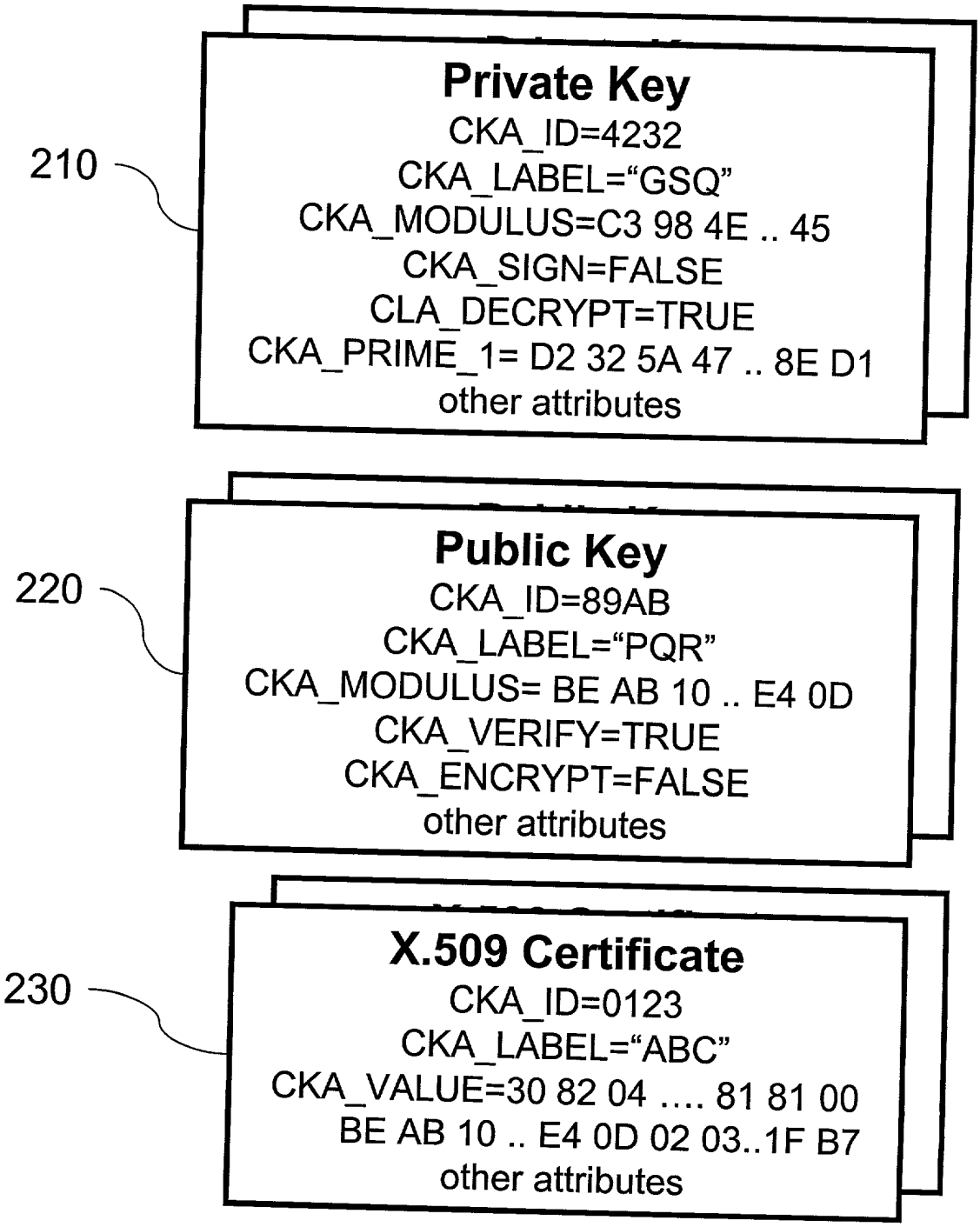
Private Key
CKA_ID=4232
CKA_LABEL="GSQ"
CKA_MODULUS=C3 98 4E .. 45
CKA_SIGN=FALSE
CLA_DECRYPT=TRUE
CKA_PRIME_1= D2 32 5A 47 .. 8E D1
other attributes
210
Public Key
CKA_ID=89AB
CKA_LABEL="PQR"
CKA_MODULUS= BE AB 10 .. E4 0D
CKA_VERIFY=TRUE
CKA_ENCRYPT=FALSE
other attributes
220
X.509 Certificate
CKA_ID=0123
CKA_LABEL="ABC"
CKA_VALUE=30 82 04 .... 81 81 00
BE AB 10 .. E4 0D 02 03..1F B7
other attributes
230

FIG. 2

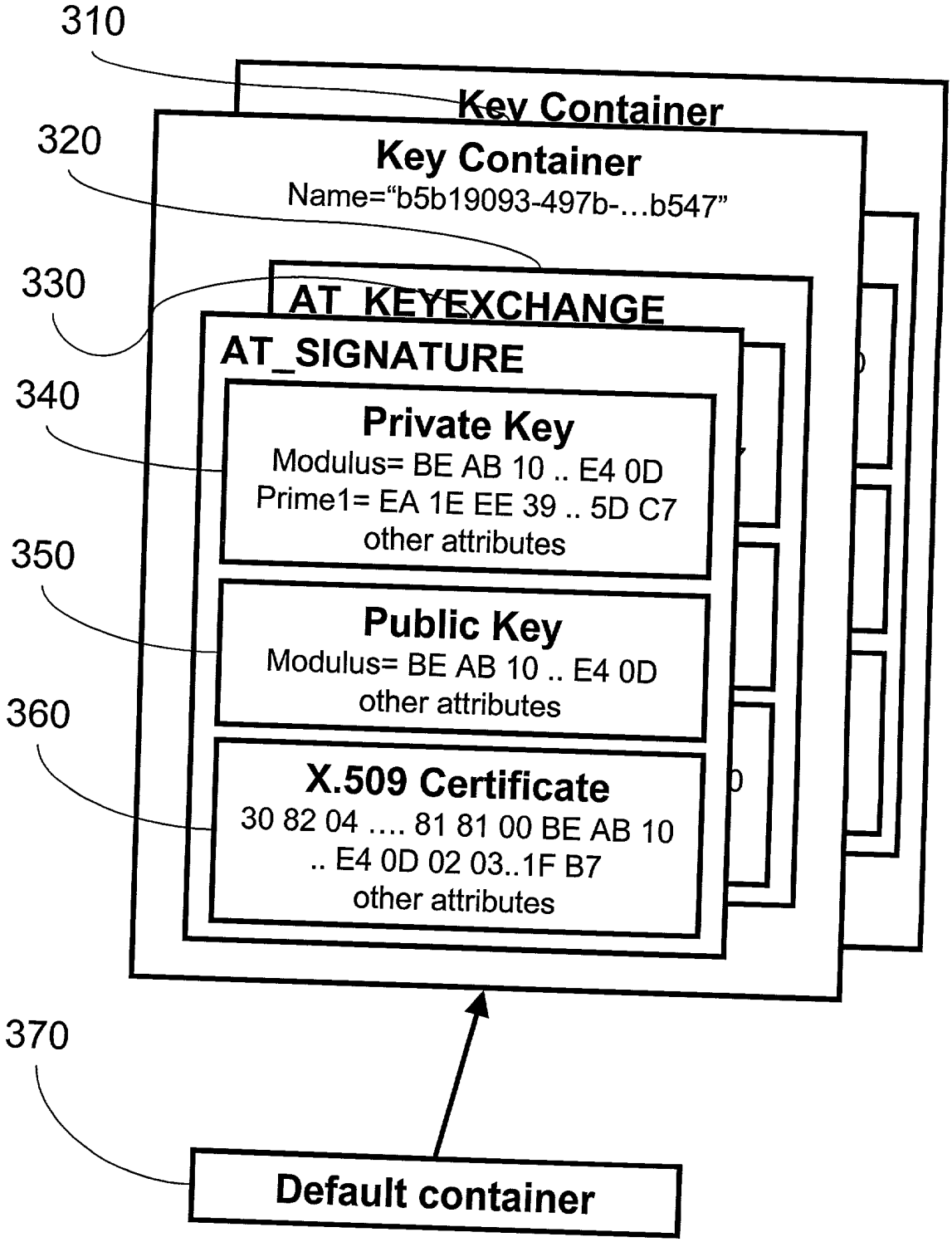
310
Key Container
320
Key Container
Name="b5b19093-497b-…b547"
330
AT_KEYEXCHANGE
AT_SIGNATURE
340
Private Key
Modulus= BE AB 10 .. E4 0D
Prime1= EA 1E EE 39 .. 5D C7
other attributes
350
Public Key
Modulus= BE AB 10 .. E4 0D
other attributes
360
X.509 Certificate
30 82 04 …. 81 81 00 BE AB 10
.. E4 0D 02 03..1F B7
other attributes
370
Default container

FIG. 3

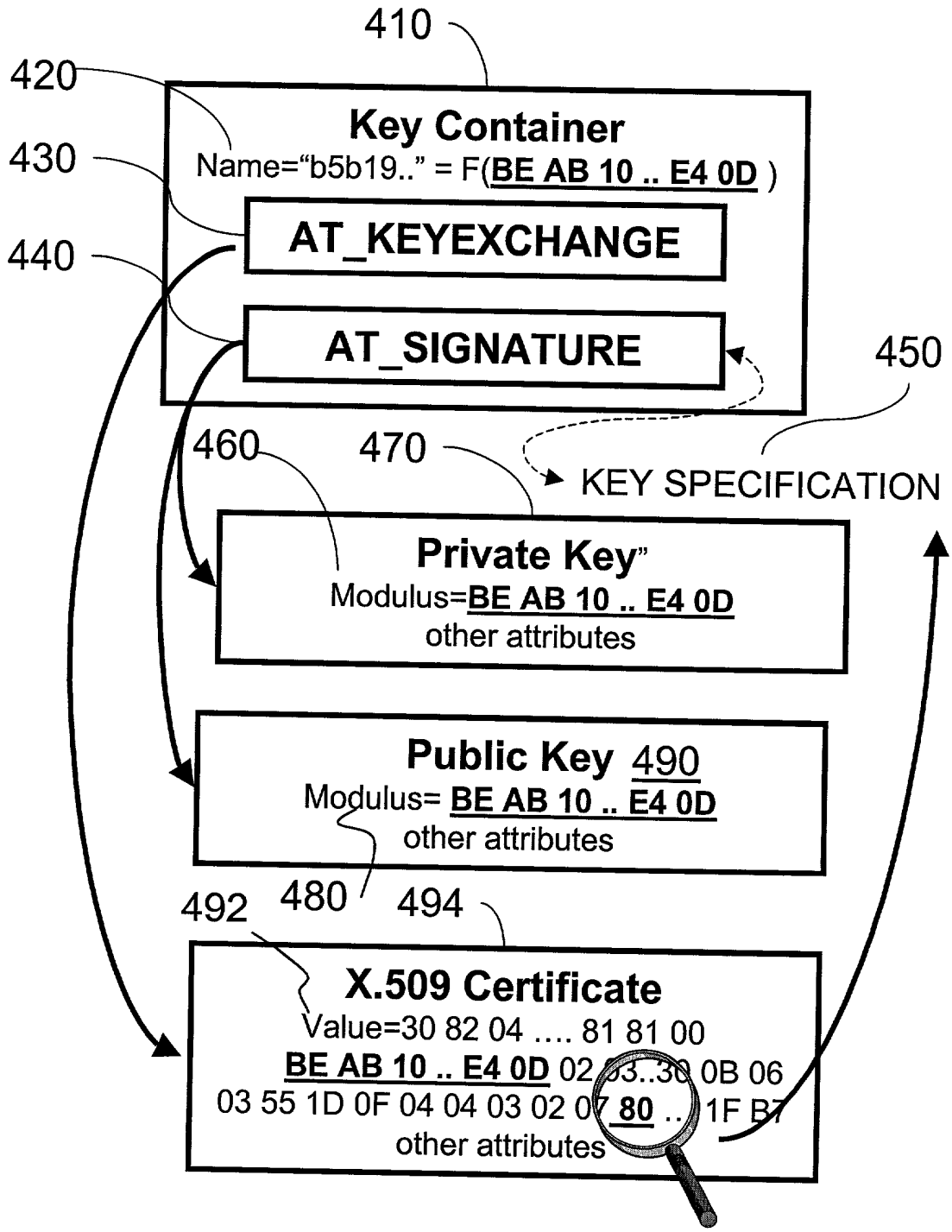
410
420
Key Container
Name="b5b19.." = F(BE AB 10 .. E4 0D)
430
AT_KEYEXCHANGE
440
AT_SIGNATURE
450
460
470
KEY SPECIFICATION
Private Key"
Modulus=BE AB 10 .. E4 0D
other attributes
Public Key 490
Modulus= BE AB 10 .. E4 0D
other attributes
492
480
494
X.509 Certificate
Value=30 82 04 .... 81 81 00
BE AB 10 .. E4 0D 02 03..30 0B 06
03 55 1D 0F 04 04 03 02 07 80 .. 1F B7
other attributes

FIG. 4

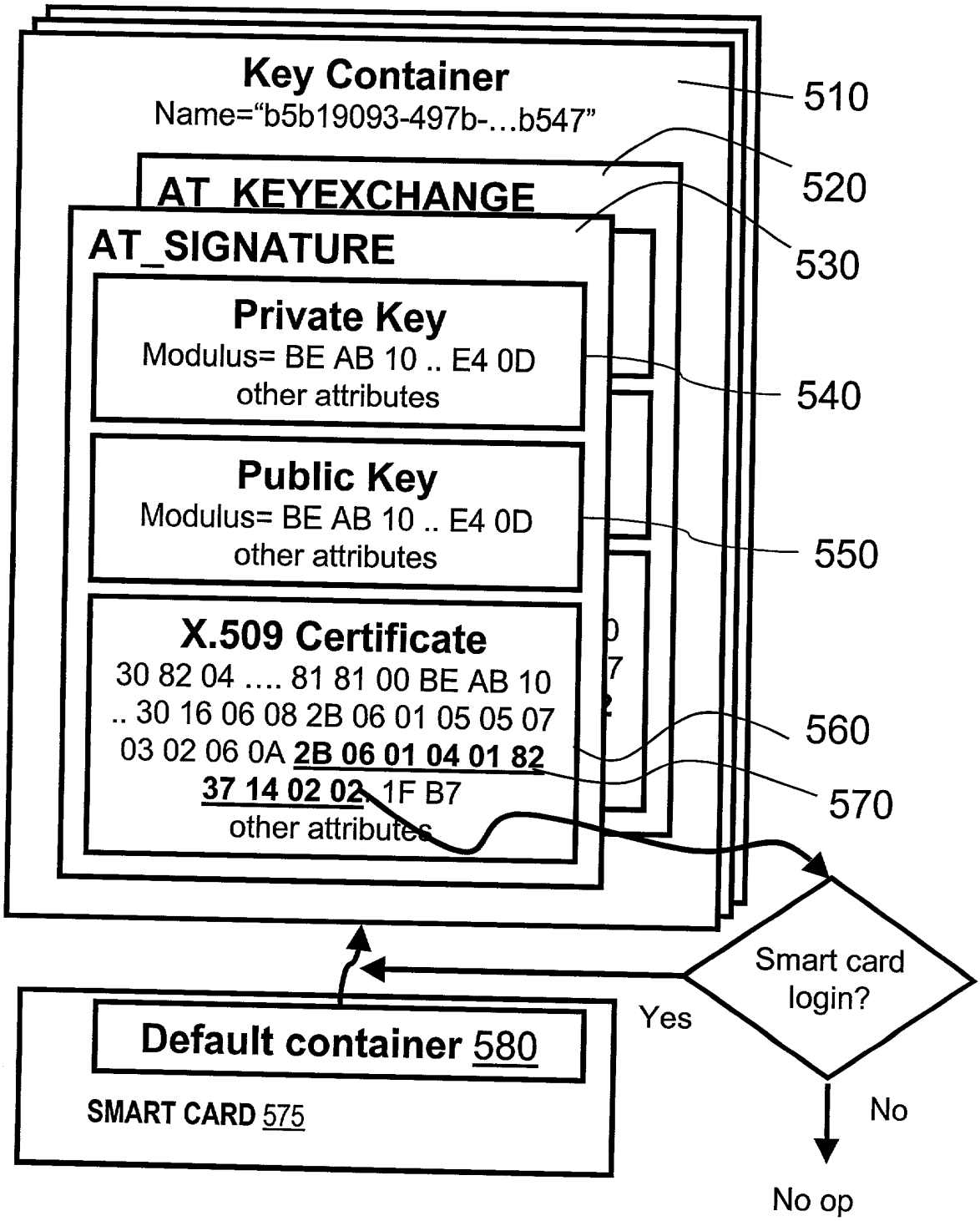
Key Container
Name="b5b19093-497b-...b547"
AT_KEYEXCHANGE
AT_SIGNATURE
Private Key
Modulus= BE AB 10 .. E4 0D
other attributes
Public Key
Modulus= BE AB 10 .. E4 0D
other attributes
X.509 Certificate
30 82 04 .... 81 81 00 BE AB 10
.. 30 16 06 08 2B 06 01 05 05 07
03 02 06 0A 2B 06 01 04 01 82
37 14 02 02 1F B7
other attributes
510
520
530
540
550
560
570
Smart card login?
Yes
No
No op
Default container 580
SMART CARD 575

FIG. 5

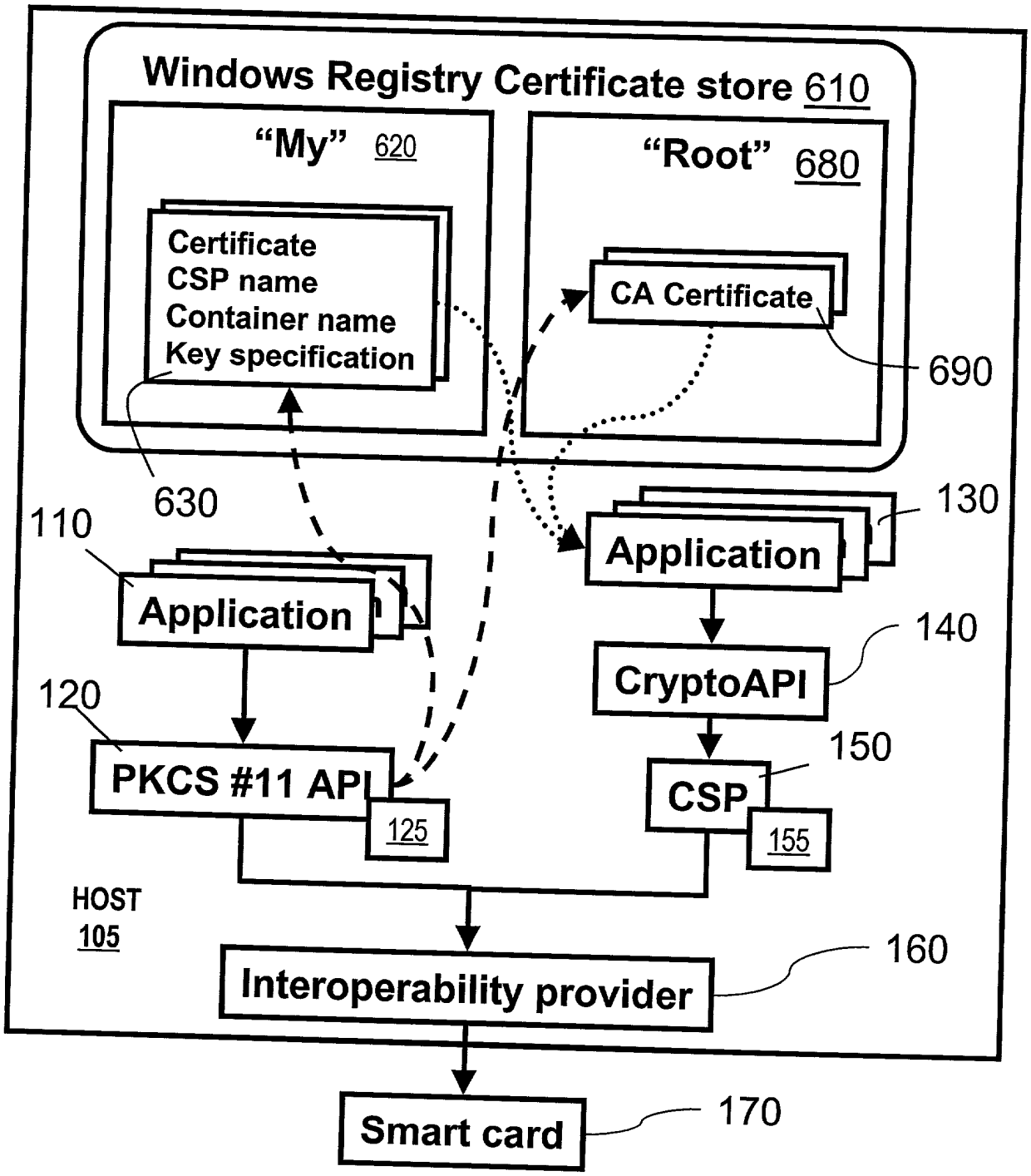
Windows Registry Certificate store 610
"My" 620
"Root" 680
Certificate
CSP name
Container name
Key specification
CA Certificate
690
630
110
130
Application
Application
140
CryptoAPI
120
150
PKCS #11 API
125
CSP
155
HOST
105
160
Interoperability provider
Smart card
170

FIG. 6

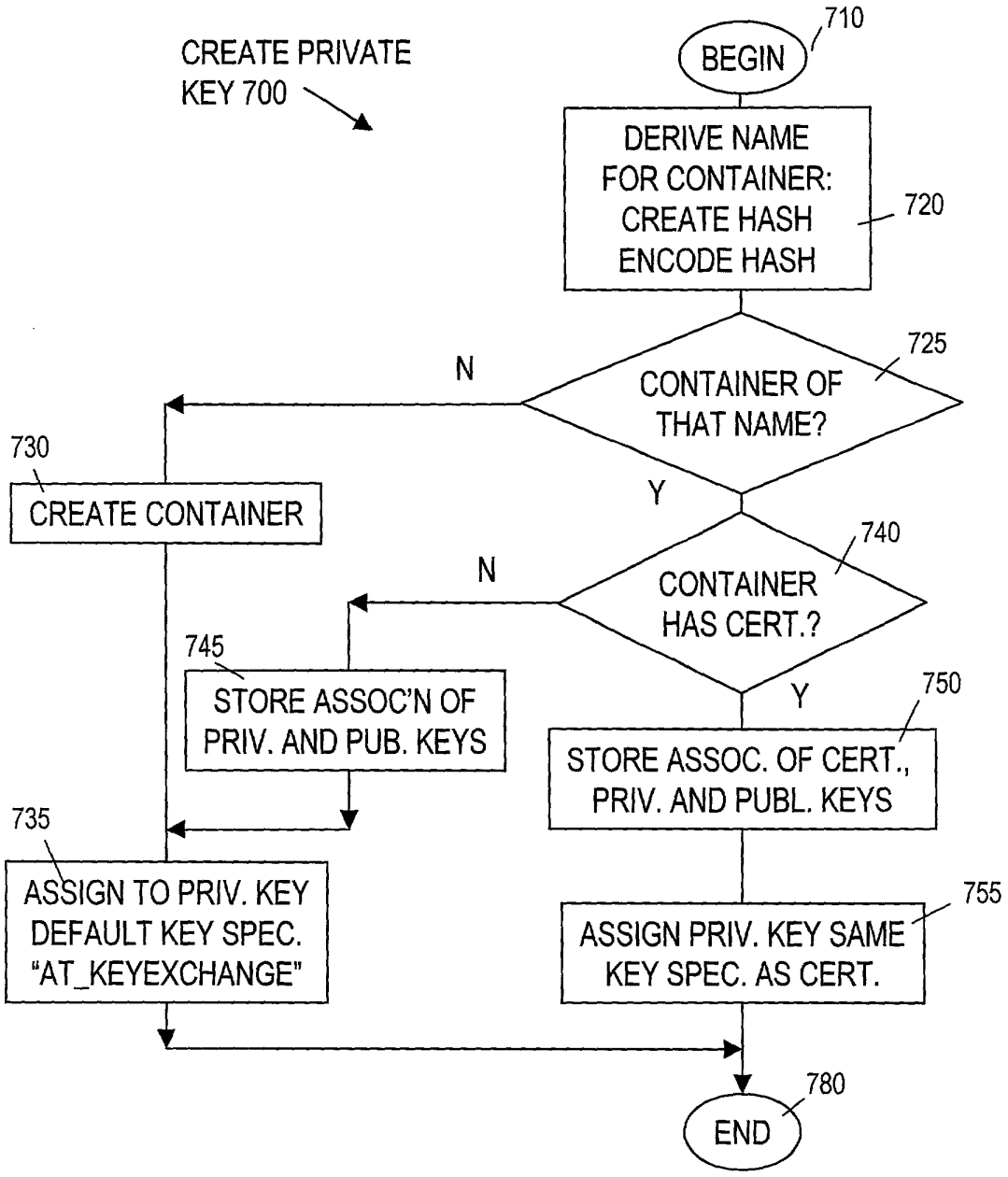
CREATE PRIVATE KEY 700
BEGIN
710
DERIVE NAME FOR CONTAINER: CREATE HASH ENCODE HASH
720
CONTAINER OF THAT NAME?
725
N
Y
730
CREATE CONTAINER
CONTAINER HAS CERT.?
740
N
Y
745
STORE ASSOC'N OF PRIV. AND PUB. KEYS
750
STORE ASSOC. OF CERT., PRIV. AND PUBL. KEYS
735
ASSIGN TO PRIV. KEY DEFAULT KEY SPEC. "AT_KEYEXCHANGE"
755
ASSIGN PRIV. KEY SAME KEY SPEC. AS CERT.
780
END

FIG. 7

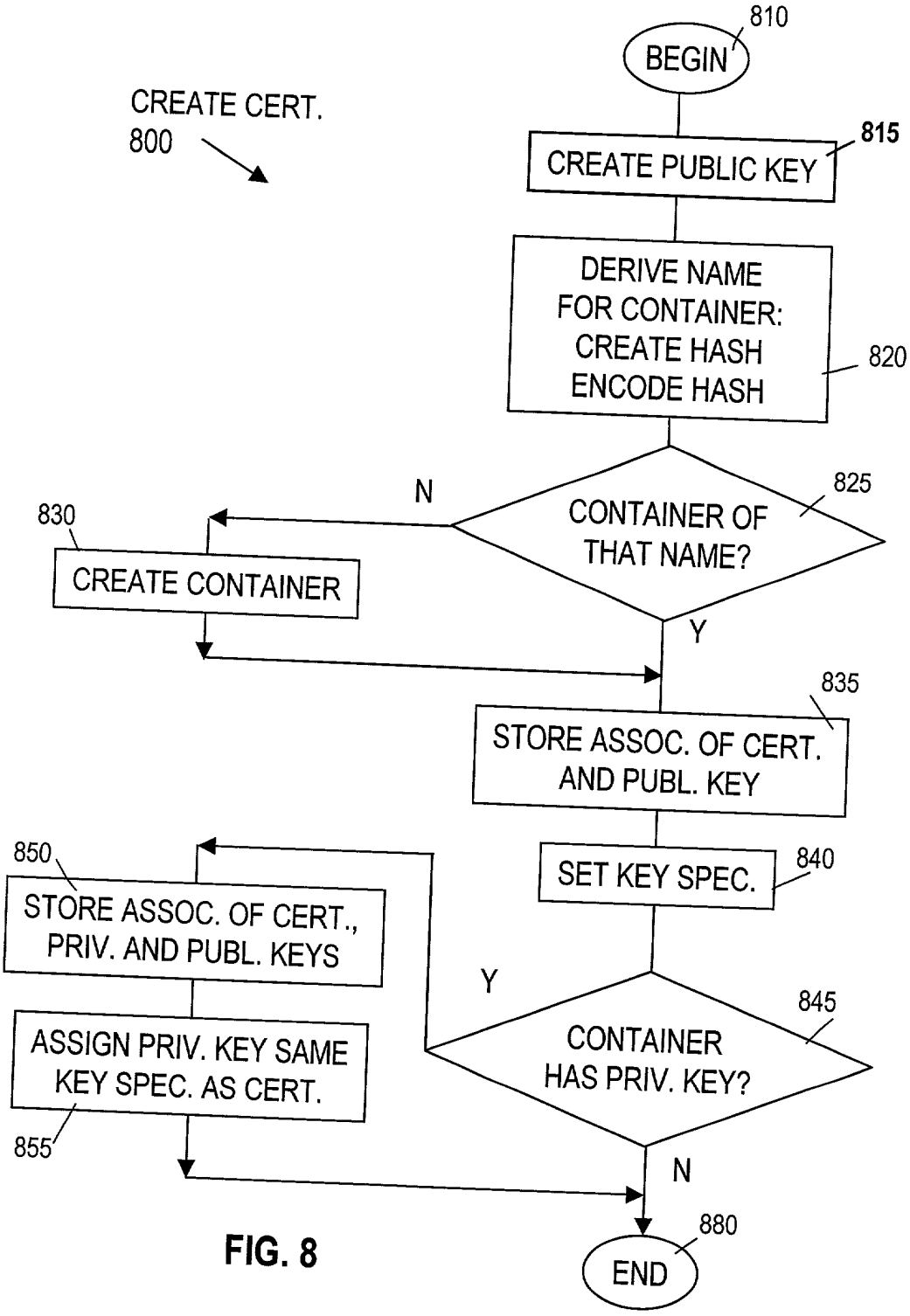
CREATE CERT.
800
BEGIN
810
CREATE PUBLIC KEY
815
DERIVE NAME FOR CONTAINER: CREATE HASH ENCODE HASH
820
CONTAINER OF THAT NAME?
825
N
Y
CREATE CONTAINER
830
STORE ASSOC. OF CERT. AND PUBL. KEY
835
SET KEY SPEC.
840
CONTAINER HAS PRIV. KEY?
845
Y
N
STORE ASSOC. OF CERT., PRIV. AND PUBL. KEYS
850
ASSIGN PRIV. KEY SAME KEY SPEC. AS CERT.
855
END
880

FIG. 8

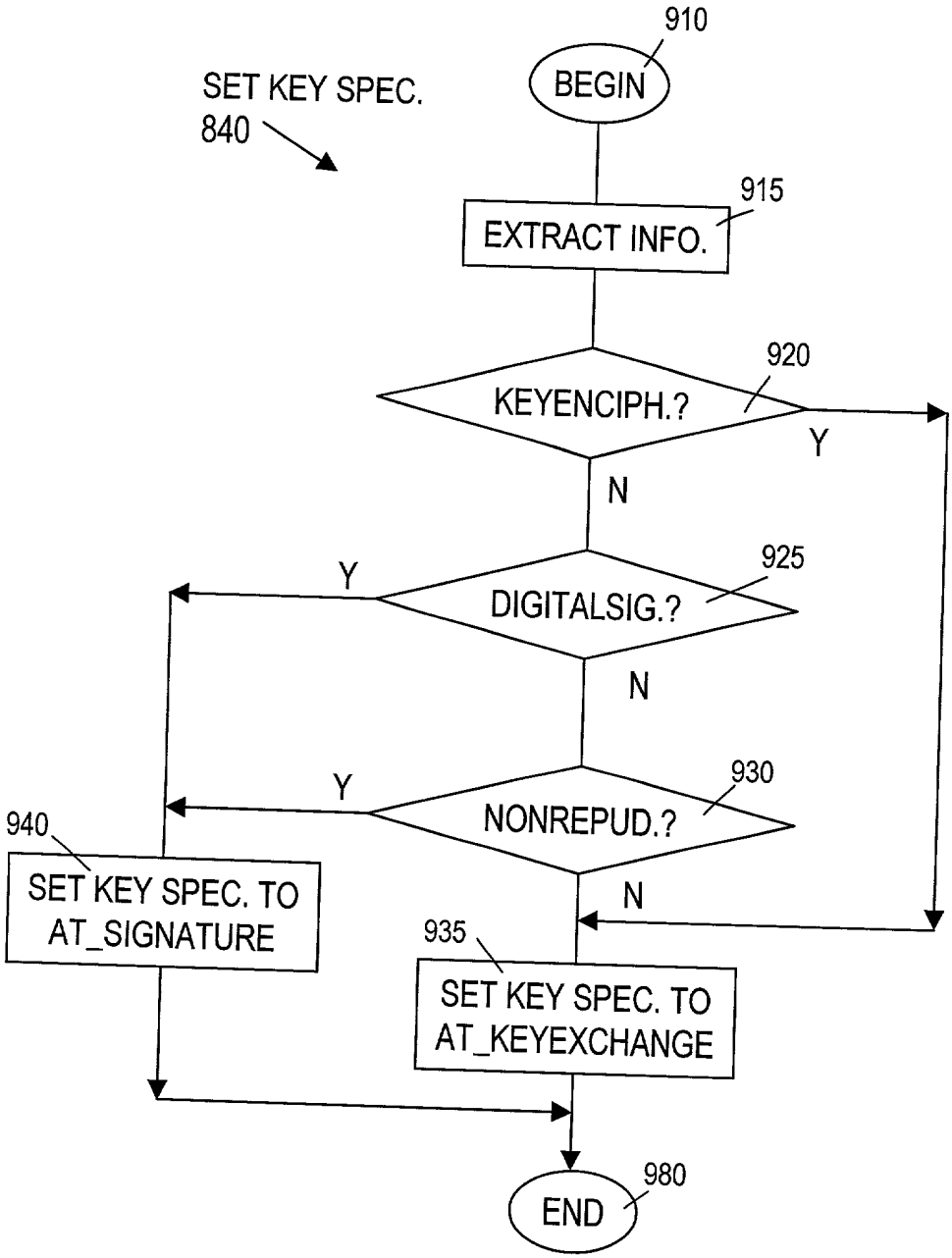
SET KEY SPEC.
840
910
BEGIN
915
EXTRACT INFO.
920
KEYENCIPH.?
Y
N
925
DIGITALSIG.?
Y
N
930
NONREPUD.?
Y
N
940
SET KEY SPEC. TO
AT_SIGNATURE
935
SET KEY SPEC. TO
AT_KEYEXCHANGE
980
END

FIG. 9

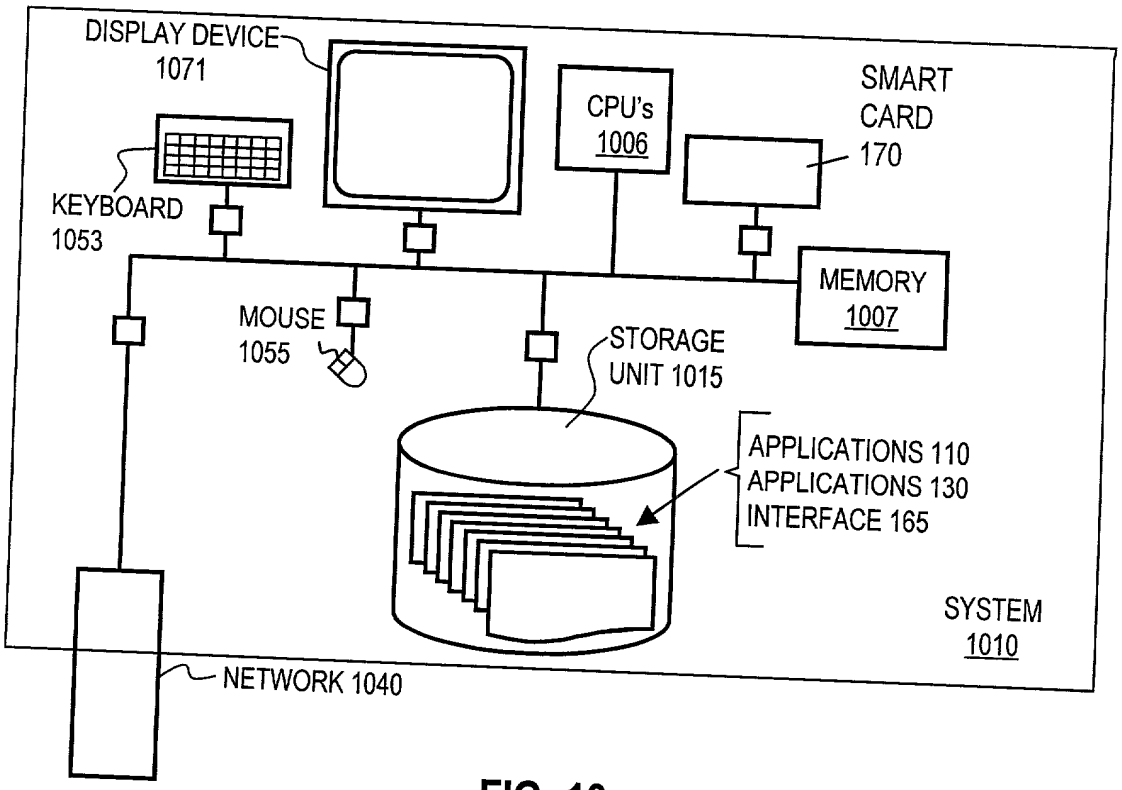
DISPLAY DEVICE
1071
CPU's
1006
SMART
CARD
170
KEYBOARD
1053
MEMORY
1007
MOUSE
1055
STORAGE
UNIT 1015
APPLICATIONS 110
APPLICATIONS 130
INTERFACE 165
SYSTEM
1010
NETWORK 1040

FIG. 10